Zmiany w ochronie danych osobowych

W maju 2018 roku nastąpi „rewolucja” w ochronie danych osobowych. Europejskie rozporządzenie o ochronie danych osobowych (RODO), które przyjęła Polska, wzmocni ochronę prywatności obywateli. Regulacja zacznie obowiązywać od 28 maja. Pozostało bardzo niewiele czasu na przygotowanie organizacji – firm, instytucji, podmiotów ekonomii społecznej - do nowego prawa. Sprawa wydaje się tym bardziej ważna, że nowe przepisy wprowadzają dość istotne zmiany w obowiązującym porządku prawnym, dotyczącym kwestii ochrony danych osobowych.

Podstawa prawna zmian

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. UE L 119 z 4 maja 2016 r.);
2. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. UE L 119 z 4 maja 2016 r.).

Unijne ogólne rozporządzenie o ochronie danych (RODO) zastąpi przepisy dotychczasowej polskiej ustawy o ochronie danych osobowych.

Cel zmian

RODO oraz ewentualne uszczegóławiające przepisy krajowe mają zapewnić osobom fizycznym nowe narzędzia ochrony swoich danych, a tym samym wzmocnić ochronę osób fizycznych.

Przepisy skończyć mają z podpisywaniem w ciemno zgód na przetwarzanie danych osobowych przez osoby składające ofertę pracy, czy podpisujące umowę abonamentową, albo zapisujące się na newsletter. Rozporządzenie będzie domagać się "od wszystkich administratorów danych, by wszelkie informacje kierowane do osób, których dane dotyczą, były formułowane jasnym i prostym językiem, by były zwięzłe i zrozumiałe. Szczególnie istotne będzie to zaś wówczas, gdy informacje i komunikaty będą kierowane do dzieci, które muszą móc je bez trudu zrozumieć" - tłumaczy Generalny Inspektor Ochrony Danych Osobowych (GIODO)[1].

Celem wprowadzenia nowej regulacji jest także ujednolicenie przepisów dotyczących ochrony danych osobowych na obszarze Unii Europejskiej. Dzięki temu zabiegowi wszystkie podmioty będą miały takie same warunki konkurencji.

Celem RODO jest także zwiększenie transparentności prowadzonej działalności zarówno przez podmioty gospodarcze, jak i administrację.

Nowe regulacje będą obowiązywać w oparciu o zasadę bezpośredniego obowiązywania prawa wspólnotowego. Tym samym nie jest konieczny proces inkorporowania tj. włączania tych przepisów do przepisów krajowych.

Zasada bezpośredniego stosowania prawa wspólnotowego – zasada, która odnosi się do sposobu i zakresu stosowania prawa wspólnotowego przez organy państwa członkowskiego.

Zasada opiera się na następujących założeniach:

- *prawo wspólnotowe jest stosowane bezpośrednio w każdym z krajów członkowskich,*
- *prawo wspólnotowe ma bezpośrednią skuteczność wobec: instytucji, podmiotów*

[1] http://tvn24bis.pl/z-kraju,74/rodo-zmiany-w-ochronie-danych-osobowych-w-2018-r,801917.html, online: 02.02.2018 r.

prawa i obywateli każdego z państw członkowskich,

- *nawet jeśli norma prawna wprowadzona do systemu prawa wspólnotowego nie została implementowana do systemu prawa krajowego, to ma ona swoje zastosowanie na terenie całej Wspólnoty, także tego kraju*[2].

Aczkolwiek nie jest konieczny proces inkorporowania prawa, to stosowanie RODO wymaga zmian w przepisach szczegółowych.

W Polsce RODO wymaga dokonania licznych zmian w ponad 130 ustawach zapewniających dostosowanie krajowego porządku prawnego do nowych norm prawnych.

Dotychczas państwami, w których już uchwalono przepisy wdrażające rozporządzenie 2016/679 są jedynie Niemcy i Austria.

Podstawowe definicje według nowego prawa

- **Dane osobowe** - dane, które oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą");
- **Możliwa do zidentyfikowania osoba fizyczna** - osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
- **Dane genetyczne** - dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;
- **Dane biometryczne** - dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub

[2] https://pl.wikipedia.org/wiki/Zasada_bezpo%C5%9Bredniego_stosowania_prawa_wsp%C3%B3lnotowego, online: 02.02.2018 r.

behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;

- **Dane dotyczące zdrowia** - dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;
- **Przetwarzanie danych osobowych** - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
- **Szczególne kategorie danych osobowych** - pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby;
- **Naruszenie ochrony danych osobowych** - naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Zasadnicze zmiany w ochronie danych osobowych

Rozporządzenie to największa zmiana w podejściu do ochrony danych osobowych od dwudziestu lat. RODO wprowadza dużo nowości, do których warto się przygotować. Poniżej charakterystyka najistotniejszych zmian.

1. **Nowe i rozszerzone prawa obywateli**

Przepisami RODO wprowadzone zostaje: „prawo do bycia zapomnianym", skierowane do obywateli, którzy życzą sobie, by ich dane osobowe zostały usunięte, uprawnienie do żądania przeniesienia danych oraz wzmocnione prawo dostępu i wglądu obywatela w jego dane.

Główny Inspektor Danych Osobowych tłumaczy, że z prawa do bycia zapomnianym skorzystamy w sytuacji, w której chcemy, by nasze dane nie były przetwarzane, a na przykład określona instytucja czy firma nie mają podstawy do takiego przetwarzania. Jak zauważa Komisja Europejska "narzędzie to ma chronić prywatność osób, niekoniecznie umożliwiać usuwanie informacji z przeszłości albo ograniczanie wolności prasy"[3].

Osoby, których dane dotyczą, będą także miały rozszerzone prawo sprzeciwu wobec przetwarzania ich danych, w tym prawo do zakazania marketingu bezpośredniego z wykorzystaniem danych osobowych, co ma niebagatelne znaczenie dla firm bazujących na analityce danych.

Jedną z istotniejszych zmian, jakie wprowadzi RODO, jest prawo do bycia zapomnianym, czyli ostatecznego i nieodwołalnego usunięcia danych osobowych z baz danych na żądanie zainteresowanego. Obecnie prawo do bycia zapomnianym dotyczy w zasadzie wyłącznie wyszukiwarek internetowych i nie opiera się na powszechnie obowiązujących przepisach, a na wyroku Trybunału Sprawiedliwości Unii Europejskiej[4].

2. Zgody

Przepisami RODO zostają wprowadzone nowe lub uzupełnione zasady uzyskiwania ważnych i weryfikowalnych zgód na przetwarzanie danych osobowych od osób, których dane dotyczą.

Nowością jest określenie po raz pierwszy zasad przetwarzania danych biometrycznych

[3] https://www.forbes.pl/biznes/zmiany-przepisow-o-ochronie-danych-giodo-komentuje/b1r458t, online: 02.02.2018 r.

[4] http://tvn24bis.pl/z-kraju,74/rodo-zmiany-w-ochronie-danych-osobowych-w-2018-r,801917.html, online: 02.02.2018 r.

(takich jak wizerunek twarzy czy odciski palców) w zatrudnianiu, w sektorze bankowym i ubezpieczeniowym. Dane takie będą mogły zostać pozyskane przez bank oraz ubezpieczycieli celem weryfikacji tożsamości klientów. W przypadku zatrudnienia, przetwarzanie przez pracodawcę danych biometrycznych obejmować ma tylko dane osobowe pracownika, jeśli dotyczą one stosunku pracy i pracownik wyrazi na to zgodę[5].

3. **Rozbudowanie obowiązku informacyjnego**

Przepisy RODO wskazują liczne informacje, które muszą być uwzględnione w komunikacji sposobu przetwarzania danych osobowych kierowanej do osób, których dane dotyczą.

4. **Ograniczenia profilowania**

Profilowanie, czyli zbieranie informacji o osobach oglądających oferty w internecie, czy szukających tradycyjnie jakiegoś towaru czy usługi, nie będzie zakazane. Jednak osoby profilowane będą musiały zostać poinformowane nie tylko o tym, że są obiektem zainteresowania algorytmów marketingowych, ale również o konsekwencjach z tego wynikających. Wprowadzony zostanie obowiązek otrzymania zgody na profilowanie przed rozpoczęciem zbierania danych, surowy obowiązek informowania o profilowaniu oraz konieczność akceptacji braku zgody na profilowanie.

5. **Bezpośrednia odpowiedzialność przetwarzającego dane**

Organizacje przetwarzające dane osobowe pochodzące z innych firm, w trakcie świadczenia usług na ich rzecz (jak na przykład firmy dostarczające rozwiązania w chmurze czy firmy hostingowe), będą ponosić bezpośrednią odpowiedzialność za złamanie zapisów RODO, włączając w to ryzyko otrzymania kary finansowej. Co więcej będą wymagane bardziej restrykcyjne niż dotychczas obowiązki w zakresie tworzenia umów o przetwarzaniu, natomiast odszkodowania i ograniczenia odpowiedzialności najprawdopodobniej będą podlegać renegocjacji.

6. **Obowiązkowa inwentaryzacja danych i wymagania związane z dokumentacją**

[5] http://tvn24bis.pl/z-kraju,74/rodo-zmiany-w-ochronie-danych-osobowych-w-2018-r,801917.html, online: 02.02.2018 r.

Kontrolujący i przetwarzający dane będą zobowiązani od przygotowania i utrzymania wszechstronnych rejestrów dotyczących przetwarzanych danych, uwzględniających m.in.: powody przetwarzania danych, kategorie podmiotów danych i danych osobowych, adresatów danych, rejestry międzynarodowych transferów danych, rejestry naruszeń i incydentów, rozwój i utrzymanie zasad ochrony prywatności dla każdej linii produktowej, przechowywanie potwierdzonych zgód na przetwarzanie danych itd.

7. Ocena wpływu ochrony danych

Wykonanie takiej analizy będzie obowiązkowe przed podjęciem działań „wysokiego ryzyka", takich jak na przykład profilowanie na dużą skalę czy wykorzystanie danych szczególnych kategorii (takich jak dane dotyczące zdrowia).

8. Zgłaszanie naruszeń

Obowiązkiem administratorów danych będzie zgłaszanie w ciągu 72 godzin od wykrycia do właściwego organu nadzoru przypadków naruszeń, które mogą skutkować zagrożeniem praw i swobód osób, których dane zostały naruszone. Może także wystąpić konieczność zawiadomienia konkretnej osoby, bez zbędnej zwłoki, o przypadku wystąpienia dużego ryzyka naruszenia jej praw lub swobód.

9. Wyznaczenie Inspektora Ochrony Danych Osobowych

Nowa regulacja przewiduje wprowadzenie do systemu ochrony danych osobowych nowego podmiotu tj. Inspektora Ochrony Danych w miejsce funkcjonującego obecnie Administratora Bezpieczeństwa Informacji. Funkcja taka pojawi się w podmiotach publicznych oraz organizacjach, których główna działalność wiąże się z przetwarzaniem danych osobowych w dużej skali. Inspektor musi dysponować wiedzą ekspercką w zakresie ochrony danych osobowych.

10. Rejestr danych

Rozporządzenie znosi obowiązek zgłaszania rejestru danych do organów ochrony danych o przetwarzaniu danych (w Polsce: Główny Inspektor Ochrony Danych Osobowych). Do tej instytucji będą jednak musiały być zgłaszane przypadki naruszenia danych osobowych.

Przygotowanie do zmian

Administratorzy danych osobowych - firmy czy organizacje pozarządowe - muszą dostosować bazy danych do przepisów RODO. Między innymi muszą sprawdzić dotychczasowe rozwiązania z zakresu ochrony danych osobowych i w wielu przypadkach je zmodyfikować.

Konieczne jest przeszukanie wszystkich zasobów teleinformatycznych, co będzie nie lada wyzwaniem, gdyż dane mogą być nie tylko w bazach, ale również w plikach tekstowych zlokalizowanych na komputerach użytkowników, plikach ze skanami dokumentów itp.[6]

Niestosowanie się do nowych zasad przetwarzania danych osobowych może m.in. skutkować odpowiedzialnością finansową – administracyjnymi karami pieniężnymi nawet do 20 milionów euro lub 4 proc. całkowitego rocznego światowego obrotu.
Niezależnie od tego osoba, której prawa zostały naruszone, może też dochodzić swoich roszczeń przed sądem cywilnym.
Z drugiej strony, wejście w życie nowych przepisów wymusi ułatwienia, oszczędności i rozwój innowacyjności.
Główny Inspektorat Ochrony Danych Osobowych prowadzi cykl warsztatów, które mają przygotować do nadchodzących zmian administratorów danych osobowych.

Opracowała: Iwona Raszeja-Ossowska

Tekst ma charakter informacyjno –edukacyjny.
Nie jest opinią prawną.

Źródła:

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. UE L 119 z 4 maja 2016 r.),

[6] Tamże.

2. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. UE L 119 z 4 maja 2016 r.).
3. https://blog-daneosobowe.pl/czym-sa-dane-osbowe-wg-rodo/, online: 02.02.2018 r.
4. http://tvn24bis.pl/z-kraju,74/rodo-zmiany-w-ochronie-danych-osobowych-w-2018-r,801917.html, online: 02.02.2018 r.
5. http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016R0679&from=PL, online: 02.02.2018 r.
6. https://www.forbes.pl/biznes/zmiany-przepisow-o-ochronie-danych-giodo-komentuje/b1r458t, online: 02.02.2018 r.
7. https://pl.wikipedia.org/wiki/Zasada_bezpo%C5%9Bredniego_stosowania_prawa_wsp%C3%B3lnotowego, online: 02.02.2018 r.